Audit Report

YEAR 2000 COMPUTING ISSUES RELATED TO THE DEFENSE AUTOMATIC ADDRESSING SYSTEM CENTER

Report No. 99-082 February 18, 1999

Office of the Inspector General
Department of Defense

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Year 2000 Computing Issues Related to the Defense Automatic Addressing System Center

B. DATE Report Downloaded From the Internet: 09/02/99

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #): **OAIG-AUD (ATTN: AFTS Audit Suggestions)**
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ **Preparation Date 09/02/99**

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.

Additional Copies

To obtain additional copies of this audit report, contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or FAX (703) 604-8932 or visit the Inspector General, DoD Home Page at: www.dodig.osd.mil.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Planning and Coordination Branch of the Audit Followup, and Technical Support Directorate at (703) 604-8908 (DSN 664-8908) or FAX (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil; or by writing to the Defense Hotline, The Pentagon, Washington, D.C. 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

AIS	Automated Information System
ASD (C^3I)	Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
DAAS	Defense Automatic Addressing System
DAASC	Defense Automatic Addressing System Center
DLA	Defense Logistics Agency
DSDC	DLA Systems Design Center
FAR	Federal Acquisition Regulation
Y2K	Year 2000

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202

February 18, 1999

MEMORANDUM FOR DIRECTOR, DEFENSE LOGISTICS AGENCY

SUBJECT: Audit Report on the Year 2000 Computing Issues Related to the Defense Automatic Addressing System Center (Report No. 99-082)

We are providing this report for information and use. This is one in a series of reports being issued by the Inspector General, DoD, in accordance with an informal partnership with the Chief Information Officer, DoD, to assess progress made by DoD Components who are preparing information technology systems for year 2000 compliance. We considered management comments on a draft of this report in preparing the final report.

Management comments on the draft of this repot conformed to the requirements of DoD Directive 7650.3, and left no unresolved issues. Therefore, no additional comments are required.

We appreciate the courtesies extended to the audit staff. Questions on the audit should be directed to Mr. Raymond D. Kidd at (703) 604-8828 (DSN 664-8828) (rkidd@dodig.osd.mil) or Mr. Hassan A. Soliman at (703) 604-8868 (DSN 664-8868) (hsoliman@dodig.osd.mil). See Appendix D for the report distribution. The audit team members are listed inside the back cover.

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 99-082
(Project No. 9LD-9021.01)

February 18, 1999

Year 2000 Computing Issues Related to the Defense Automatic Addressing System Center

Executive Summary

Introduction. This is one in a series of reports being issued by the Inspector General, DoD, in accordance with an informal partnership with the Chief Information Officer, DoD, to monitor DoD efforts to address the year 2000 computing challenge. For a complete listing of audit projects, see the year 2000 webpage on the IGnet at http://www.ignet.gov.

Objectives. The audit objective was to evaluate whether the Defense Logistics Agency was adequately planning for and managing year 2000 conversions to avoid undue disruption to its supply mission. Specifically, for this segment of the audit, we reviewed year 2000 risk assessments and testing and contingency plans at the Defense Automatic Addressing System Center (DAASC) for systems that support the supply mission.

Results. The Defense Logistics Agency and DAASC have recognized the importance of the year 2000 issue and have taken positive actions to identify and correct year 2000 problems in automated information systems. However, further action was needed to improve the DAASC contingency plan and incorporate Federal Acquisition Regulation year 2000 requirements in contracts for automated information systems to ensure that the Defense Logistics Agency will be able to perform its core supply mission without interruption. Those additional actions should be undertaken immediately to minimize the risk of mission disruption. See the finding section of this report for details.

Summary of Recommendations. We recommend that the Director, DAASC, prepare contingency plans according to the requirements and guidelines in the DoD Year 2000 Management Plan and include Federal Acquisition Regulation year 2000 compliance language in all open contracts.

Management Comments. The Director, Defense Logistics Agency concurred with the recommendations, stating that DAASC now includes data preservation and workarounds in its contingency plan. The workarounds include identifying alternatives to DAASC for submitting requisitions for supply items. DAASC also incorporated Federal Acquisition Regulation year 2000 requirements in all affected contracts before January 31, 1999. See finding for a summary of management comments and management comments section of report for the complete text of management comments.

Table of Contents

Background

Because of the potential failure of computers to run or function throughout the Government, the President issued Executive Order 13073, "Year 2000 Conversion," February 4, 1998, making it policy that Federal agencies ensure that no critical Federal program experiences disruption because of the year 2000 (Y2K) problem. The order requires that the head of each agency ensure that efforts to address the Y2K problem receive the highest priority attention in the agency.

A Secretary of Defense memorandum, "Year 2000 (Y2K) Compliance," August 7, 1998, stated that DoD is making insufficient progress in its effort to solve its Y2K computer problem. The memorandum directed more accountability and reporting requirements at the highest levels within DoD. The memorandum further stated that if Y2K progress was still lagging in November and December 1998, all further modifications to software, except those needed for Y2K remediation, would be prohibited after January 1, 1999. Additionally, the memorandum requires DoD Components to ensure that funds are not obligated for any information technology contract that processes date-related information that does not contain Y2K requirements specified in the Federal Acquisition Regulation (FAR).

A Deputy Secretary of Defense memorandum, "Year 2000 (Y2K) Verification of National Security Capabilities," August 24, 1998, placed responsibility for Y2K issues with each Principal Staff Assistant of the Office of the Secretary of Defense and required that all acquisition of information technology be Y2K-compliant. Specifically, the memorandum stated that each Principal Staff Assistant must verify that all functions under his or her purview will continue unaffected by Y2K issues. The memorandum further required that the designated Principal Staff Assistant provide plans for Y2K-related end-to-end testing of each process within five functional areas, including logistics, to the Deputy Secretary of Defense by November 1, 1998. The Principal Staff Assistant for Logistics is the Under Secretary of Defense (Acquisition and Technology), who relies on the Deputy Under Secretary of Defense (Logistics), and, in turn, the Director for Logistics System Modernization, to lead the logistics community Y2K efforts.

Defense Automatic Addressing System Center Mission and Functions. The Defense Automatic Addressing System Center (DAASC), a component of the Defense Logistics Agency (DLA), is a supply and distribution support service that processes over 1 billion logistics transactions each year to over 177,000 customers worldwide. The function of DAASC is to electronically edit and route logistics

transactions and compile financial, logistical, and procurement data. Its functions improve the accuracy of logistics data and decrease work load for its customers.

Y2K Responsibilities for the Defense Automatic Addressing System Center. DAASC is responsible for correcting its Automated Information Systems (AISs) that do not comply with Y2K requirements. Each month, DAASC submits Y2K status reports to the DLA Systems Design Center (DSDC). DSDC reviews and consolidates reports from all DLA components, and submits the consolidated report to the Chief Information Office, DLA. The Chief Information Office reviews and submits the report to the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (ASD [C^3I]) for submission to the Office of Management and Budget. A program office at the DSDC manages the Y2K solutions for applications under its configuration management control. The program scope includes DSDC application programs and commercial-off-the-shelf products (computer hardware and software) used by the applications.

Objectives

The audit objective was to evaluate whether DLA was adequately planning for and managing Y2K conversion. Specifically, in this segment of the audit, we reviewed Y2K risk assessments and testing and contingency plans for the DAASC systems that support the core supply mission. See Appendix A for a discussion of the audit scope and methodology and for a summary of prior coverage.

Status of the Defense Automatic Addressing System Center Year 2000 Program

The DLA and DAASC have taken positive actions to identify and correct Y2K problems with DAASC AISs. However, the DAASC contingency plan needed to address alternative procedures for continuity of operations of its core mission and to describe how it would preserve data for its mission-critical AISs. DAASC also needed to include the FAR Y2K-compliance language in its information technology contracts. Such actions were needed immediately to ensure that DLA would be able to perform its core supply mission without interruption after the year 1999.

Automated Information Systems at DAASC

The DAASC has 35 AISs located at Dayton, Ohio, and Tracy, California. Of the 35 AISs, DAASC identified 16 as mission-critical (see Appendix B). All DAASC AISs run on mainframe, minicomputer, or personal computer platforms*. Additionally, DAASC AISs interface with 50 external systems owned by DoD Components and other Federal agencies (see Appendix C).

Of the 35 DAASC AISs, 25 do not process dates or have date fields and 10 do process dates. Of the 25 that do not process dates, 13 are mission-critical. Of the 10 AISs that process dates, 3 could have a critical impact on mission performance. The three critical systems are the Defense Program for the Reutilization of Assets, Defense Automated Addressing System (DAAS) Master Routing System, and the DAAS Network Control System.

* Mainframes are large computers capable of supporting thousands of users simultaneously. Minicomputers are mid-size computers that, in general, are multiprocessing systems capable of supporting up to about 200 users simultaneously. Personal computers are small computers designed for individual users.

Actions Taken to Correct the Year 2000 Problem

The DLA and DAASC took positive actions to identify and to correct Y2K problems that the DAASC AISs had. DLA:

- appointed a DLA program manager, responsible to the chief information officer, for properly assessing and testing DAASC AISs to ensure validation of the systems for certification.
- designated a DAASC executive office with final oversight of the DAASC Y2K compliance strategy, test plan, and test report.
- tasked the DAASC Systems Engineering Directorate with project planning, tracking, and quality assurance; contract and configuration management; and managing the Y2K compliance and certifying process.
- tasked the DAASC Program Management Office to establish the functional requirements for the DAASC Y2K certifications and to coordinate Y2K compliance certificates. The DAASC Program Management Office will also create the test data for the Y2K tests.
- tasked DAASC to test application programs and AISs to verify their compliance with Y2K.

DAASC took the following actions to correct Y2K problems. It:

- executed memorandums of agreement with its customers for AIS interfaces to address methods of data exchange between systems, entity responsibilities for modifying interfaces, and milestones for modifying interfaces. Those interface agreements and associated documents met the requirements identified in the DoD Year 2000 Management Plan (the DoD Management Plan).
- reviewed the programming logic for its AISs and identified 25 AISs that did not process dates. All 25 AISs, operated on computer platforms that were Y2K-compliant. For those AISs, which included 13 mission-critical AISs, DAASC prepared documentation for Y2K certification and DLA certified those systems as Y2K-compliant. As part of the certification process, DAASC obtained documentation from vendors or their websites that the commercial-off-the-shelf

products operating on DAASC AISs were Y2K-compliant. The DoD Management Plan allowed DoD Components to accept vendor documentation of Y2K compliance in lieu of testing.

- developed a plan for testing its AISs that process dates and engaged the services of an independent contractor to oversee testing procedures and results. DAASC planned to test its 10 AISs that process dates and to submit certification documents for those systems to DLA Headquarters by December 31, 1998. The tests are planned to address Y2K concerns at both application and system levels. At the application level, DAASC planned to test date projections and leap years. At the system level, DAASC planned to test the interoperability of its systems. Plans for testing the interoperability of DAASC AISs with customer AISs will be developed at the DLA Headquarters level. Subsequently, DLA informed us that all DAASC AISs were certified Y2K-compliant.

- updated its October 1997 Y2K contingency plan. However, improvements were needed to address requirements in the DoD Management Plan.

Preparing AIS Contingency Plan

The DAASC draft contingency plan did not fully address the DoD Management Plan requirements and guidelines for risk management and contingency planning. The DAASC contingency plan needed to address alternative procedures for continuity of operations of the DAASC core mission and to describe how DAASC would preserve data for its mission-critical AISs. Improving the draft DAASC contingency plan would assist in ensuring continuity of the DAASC business operations if a Y2K problem occurs.

DoD Management Plan. The DoD Management Plan contains requirements, guidelines, and recommendations for DoD Components related to the Y2K problem and to the development of contingency plans. It states that system level contingency planning is the primary management tool to prepare for unanticipated disruptions. The DoD Management Plan requires the development of a contingency plan for mission-critical AISs assigned priority one. Priority one systems include any mission-critical system that affects the safety and well-being of personnel. Further, it states that contingency plans should identify risks that could cause system failures, identify ways to preserve system data, establish emergency

contingency plans, and establish "zero date" strategy and procedures. Triggers are mechanisms that activate the contingency plan and the zero date is the period December 30, 1999, through January 1, 2000. The DoD Management Plan also states that contingency planning associated with risk management actions may be incorporated into a formal risk management plan or into system-level contingency plans.

DAASC Contingency Plan. The draft DAASC contingency plan needed improvement in addressing workarounds and data preservation. For example, the plan did not contain alternative procedures for working around system failures nor describe how DAASC would preserve data, such as backing up the systems. Workarounds and data preservation would better ensure continuation of the DAASC core mission without interruption. However, the draft contingency plan did identify risks associated with AIS failures, contingency plan triggers, and a zero date strategy.

Workaround Procedures. DAASC did not include workarounds in its contingency plan because it believed that Y2K problems, should they occur, would be no different than other AIS problems that occurred at DAASC. DAASC handled those problems by contacting staff through pagers. Those contacts were accomplished through a management system, Multi-Vendor Automated Expert Manager, that monitored DAASC processing platforms. When problems surfaced, the Multi-Vendor Automated Expert Manager automatically notified appropriate personnel through their pagers. Additionally, DAASC planned to have a team consisting of functional and technical personnel on-site during the change from the year 1999 to the year 2000. The team will review files, journals, logs, and other pertinent data to evaluate any adverse impact on DAASC processing during the change. Although the DAASC plans for fixing AIS problems appear adequate, the plans did not address how customers would be able to submit requisitions through the DoD supply system until DAASC fixes its AISs. For example, the contingency plan could contain instructions on how DAASC customers should reroute requisitions to supply sources should an AIS at DAASC fail.

Data Preservation. DAASC did not include data preservation procedures in its contingency plan because DAASC officials were not aware of the requirement. As part of its operations, however, DAASC copied its databases each week and backed up its critical files every day. Including its procedures in the contingency plan would ensure that the staff was aware of the need to preserve data near the zero date and the DAASC procedures to preserve data.

Importance of Contingency Planning. The DoD Management Plan states that even systems that have been renovated and tested could fail, and the failure of one system could disrupt many others. If DAASC AISs failed, the DLA supply

mission could be interrupted. For example, DAASC could lose communications with 50 external interfaces and interfaces within its own AISs. It also could lose data that could not be replaced. Because DAASC could not provide assurance that it would quickly fix Y2K problems, contingency planning is a critical element that would ensure that DLA would be able to perform its core supply mission without interruption after the year 1999.

Management Action Taken. After we inquired about the contingency plan, a DLA official advised us that DAASC revised its draft contingency plan to include workarounds and data preservation procedures, and was reviewing the revised plan. The changes to the DAASC contingency plan included procedures to notify DAASC customers of how to submit requisitions if DAASC systems break down. In the notifications, to be sent during the second and fourth quarters of calendar year 1999, DAASC planned to include the telephone numbers for the Emergency Supply Operation Center and advise customers to pre-position materials before December 31, 1999. DAASC stated that its data preservation strategy would be to copy onto computer tape all its data each week and all changes made to critical files each day In its comments on the draft report, DLA stated that DAASC included data preservation and workarounds in its updated contingency plan.

Incorporating Y2K Requirements in AIS Contracts

The DAASC did not address FAR requirements for Y2K in its information technology contracts for maintenance and software development. FAR requirements were not in DAASC contracts because the acquisition management office at the DAASC thought that the contracting office at Wright-Patterson Air Force Base would address Y2K in contracts. As a result, the DAASC did not have complete assurance that its AISs would operate properly starting in the year 2000; and it may not have recourse against vendors for computer hardware or software that are not Y2K-compliant.

FAR Requirements for Y2K Compliance. Part 39 of the FAR prescribes acquisition policies and procedures for acquiring information technology. As of January 2, 1997, part 39 has included Y2K compliance language. Specifically,

FAR, part 39 states that agencies must make sure that solicitations and contracts contain Y2K compliance language, which requires that information technology to be procured be Y2K-compliant.

ASD (C^3I) Guidance. As discussed in Inspector General, DoD, Audit Report No. 98-065, "DoD Information Technology Solicitations and Contract Compliance for Year 2000 Requirements," February 6, 1998, the ASD (C^3I) issued a memorandum, "Acquisition of Year 2000 (Y2K) Compliant Information Technology (IT) and Bringing Existing IT Into Compliance," December 18, 1997. The memorandum addressed the audit finding that many indefinite delivery type contracts for information technology did not contain the required FAR Y2K compliance language. The memorandum stated that orders for information technology shall not be placed against a contract or other acquisition instruments unless that contract or instrument requires Y2K compliance or the order itself requires Y2K compliance.

AIS Purchases. During FY 1998, neither DAASC nor its servicing contract office at Wright-Patterson Air Force Base took action to modify existing DAASC information technology contracts or address the Y2K in FY 1999 contract actions. As of July 29, DAASC had awarded 50 contract actions on 40 separate contracts for information technology. Those actions included 39 contract actions valued at $4.7 million for maintenance and 11 contract actions valued at $4.5 million, to develop computer software. Of the 25 maintenance contract actions awarded at the beginning of FY 1998, 10 were extensions of existing contracts and 15 were new contracts. The remaining maintenance contracts and software development contracts were awarded throughout FY 1998. According to an official in the DAASC Acquisition Management Office, DAASC did not include the FAR Y2K compliance language in any of the FY 1998 contracts. The DAASC also had not initially included FAR Y2K compliance language in the FY 1999 maintenance contract extensions.

Management Action Taken. After we inquired about the Y2K requirements, a DAASC Acquisition Management official immediately contacted the contracting office at Wright-Patterson Air Force Base and requested that the contracting officer include the FAR Y2K compliance language in FY 1999 renewals for maintenance contracts.

Management Action Needed. DAASC actions only partially addressed FAR requirements. Specifically, DAASC did not request that the contracting office include the FAR Y2K compliance language in other maintenance contracts or in software development contracts awarded in FY 1998 that were still open as of October 16, 1998. Those contracts included systems management and computer operations support; software development for the Logistics Metrics Analysis

Reporting System, Distribution Standard System, Plant Clearance and Redistribution Screening System, and Logistics Support Data Strategy; and enterprise management.

After we inquired about the need to include FAR compliant language in all open contracts for information technology, a DLA official advised us that DAASC was in the process of updating all open contracts. DLA also provided a schedule showing the date on which the DAASC was expecting to add FAR-compliant language to its contracts.

Importance of ASD (C^3I) Y2K Contract Requirements. Without including the ASD (C^3I) required FAR Y2K compliance language in open contract actions that should have had them initially, DAASC had no assurance that its purchased AIS products, including software were Y2K-compliant; or that contractors would be obligated to fix items found to be non-compliant. Such actions are needed to better ensure that DLA will be able to perform its core supply mission without interruption after the year 1999.

Recommendations and Management Comments

We recommend that the Director, Defense Automatic Addressing System Center:

1. Prepare contingency plans in accordance with the requirements and guidelines in the DoD Year 2000 Management Plan to include addressing workarounds and data preservation.

Management Comments. DLA concurred with the recommendation, stating that DAASC had added data preservation strategy, such as daily and weekly file backups, to its contingency plans. Also, DAASC had included workarounds in its contingency plan. The workarounds were advising customers to submit emergency requisitions through the Emergency Supply Operation Center or the DLA Emergency Supply Expert System, and pre-positioning materials before December 31, 1999. DAASC will send notifications each quarter to its customers, through the first quarter of fiscal year 2000, informing them of the contingency procedures.

2. Include Federal Acquisition Regulation year 2000 compliance language in all open contracts for the purchase of information technology products, including software.

Management Comments. DLA concurred with the recommendation, stating in comments to the draft report and in subsequent information that compliance language was included in all 40 contracts before January 31, 1999.

Appendix A. Audit Process

This report is one in a series being issued by the Inspector General, DoD, in accordance with an informal partnership with the Chief Information Officer, DoD, to monitor DoD efforts to address the Y2K computing challenge. For a listing of audit projects addressing this issue, see the Y2K webpage on IGnet at http://www.ignet.gov.

Scope

We reviewed the progress that the DAASC has made in resolving Y2K computing issues. We reviewed and evaluated contingency plans, interfaces with external AISs, testing procedures, internal reporting procedures, and contracting procedures for information technology. We interviewed Y2K management officials at DLA Headquarters, DSDC and DAASC, and acquisition management officials at DAASC. We also compared DAASC Y2K efforts to those prescribed in the June 1998 draft DoD Management Plan.

DoD-Wide Corporate Level Goals. In response to the Government Performance Results Act, DoD has established 6 DoD-wide corporate-level performance objectives and 14 goals for meeting the objectives. This report pertains to achievement of the following objective and goal.

> **Objective:** Prepare now for an uncertain future. **Goal:** Pursue a focused modernization effort that maintains U.S. qualitative superiority in key war fighting capabilities. **(DoD-3)**

DoD Functional Area Reform Goals. Most major DoD functional areas have also established performance improvement reform objectives and goals. This report pertains to achievement of the following functional area objectives and goals.

- **Information Technology Management Functional Area.**
  Objective: Become a mission partner. **Goal:** Serve mission information users as customers. **(ITM-1.2)**

- **Information Technology Management Functional Area.**
  Objective: Provide services that satisfy customer information needs.
  Goal: Modernize and integrate Defense information infrastructure. **(ITM-2.2)**
- **Information Technology Management Functional Area.**
  Objective: Provide services that satisfy customer information needs.
  Goal: Upgrade technology base. **(ITM-2.3)**

High Risk Area. In its identification of risk areas, the General Accounting Office has specifically designated risks in resolution of the Y2K problems as high. This report provides coverage of that problem.

Methodology

Audit Type, Dates, and Standards. We performed this program audit from September 1998 through January 1999 in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD. We did not use computer-processed data to perform this audit.

Contacts During the Audit. We visited or contacted individuals and organizations within DoD. Further details are available upon request.

Management Control Program. We did not review the management control program related to the overall audit objective because DoD recognized the Y2K issue as a material management control weakness in the FY 1998 Annual Statement of Assurance.

Summary of Prior Coverage

The General Accounting Office and the Inspector General, DoD, have conducted multiple reviews related to Y2K issues. General Accounting Office reports can be accessed over the Internet at http://www.gao.gov. Inspector General, DoD, reports can be accessed over the Internet at http://www.dodig.osd.mil.

Appendix B. DAASC Mission-Critical Automated Information Systems

As listed below, there are 16 mission-critical AISs associated with DAASC.

DAAS Allied Communications Procedures (DAASACP). DAASACP encompasses data patterns and narrative message routing information, and it holds communications routing criteria for the DAAS customer base. It generates the file maintenance changes necessary to deliver transactions and messages to the correct destination.

DAAS Automated Digital Network Replacement System (DARS). DARS permits customers to exchange data files with DAASC over non-Automated Digital Network communications networks such as the Defense Information System Network or another Internet Protocol network. It is an alternative communications service to customers who lose their Automated Digital Network connectivity.

DAAS Automated Message Exchange System (DAMES). DAMES is a personal computer based system used for communicating with DAAS. It gives users the capability to send and receive logistics transactions and narrative traffic using file transfer protocol transmissions for communications through wide area networks or asynchronous dial-connections.

DAAS Integrated E-mail Logistics (DIELOG). DIELOG provides small volume users e-mail access to DAAS. It provides users with the capability to submit requisitions and other military standard logistical transactions without the expense of developing and maintaining an automated capability.

DAAS Master Routing System (DMRS). DMRS maintains an on-line database containing information used to assign communications routing indicators to logistics transactions. It is fundamental to the successful editing and routing of the logistics transactions handled for DoD Components and other entities using DAASC services DMRS processes dates.

DAAS Micro Automated Routing System (DMARS). DMARS edits, verifies, routes and copies transactions that flow through the DAAS environment. During transaction processing, it applies indicators that the Logistics Information Data Services and the Logistics On-Line Tracking System use for reporting purposes.

DAAS Network Control System (DNCS). DNCS provides telecommunications interoperability and network connectivity. It provides the technical platform to transition between networks such as Automated Digital Network and Defense Data Network. DNCS processes dates.

Defense Program for the Reutilization of Assets (DEPRA). DEPRA is an on-line system to track and laterally redistribute surplus items among DoD organizations and authorized civil agencies in the continental United States and the European and Pacific theaters. DEPRA processes dates.

Distribution Standard System Bridge (DSS Bridge). The DSS Bridge translates data received from and transmitted to Service legacy systems that process both military standard and non-military standard transactions.

DoD Activity Address Directory (DoDAAD). The DoDAAD maintains the names and addresses of organizations that must be identified in the Defense Logistics Standard System. The DoDAAD records include military organizational entities that requisition, receive, or ship materiel; commercial organizations that enter into materiel and service contracts with DoD; and other Federal agencies that maintain logistics support arrangements with DoD.

Electronic Data Interchange Pass-Through (EDIPAS). EDIPAS provides an electronic gateway so DoD Components and private industry can communicate.

International Logistics Communications System (ILCS). ILCS is a DoD logistics standard system providing logistics communication services to foreign military sales countries. It allows foreign nations to exchange logistics data with the U.S. Government, the DoD logistics community, and contractors.

Master Source of Supply (MSOS). MSOS maintains the National Inventory Item Number to Source of Supply database. It ensures that military standard transactions are routed to the correct source of supply in accordance with the DoD Components logistics routing rules. The database has about 9 million records.

Mid-tier Server (MIDTIER). MIDTIER is the server side of the DAASC client and server environment. It allows dial-in and network connectivity to both DAASC sites (Dayton, Ohio, and Tracy, California) for exchange of logistics transactions and DoD database query capability.

Military Assistance Program Address Directory (MAPAD). MAPAD contains the addresses of country representatives, freight forwarders, embassy offices, and in country customers for releasing foreign military sales and military assistance program grant aid shipments, and the addresses required for transmitting related

documentation. MAPAD services are available to DoD Components and to commercial organizations with material and services contracts with DoD and foreign governments, and international organizations participating in the Foreign Military Sales or military assistance grant aid programs.

Standard Point Location Code (SPLC). SPLC is a DAASC database of National Motor Freight Traffic Association codes. The SPLC supports the Military Traffic Management Command and the Defense Transportation Payment Program.

Appendix C. External Automated Information Systems That Interface With DAASC

As listed below, there are 50 AISs that interface with DAASC. All external interfaces are connected through the DAAS Network Control System, which provides network interoperability and connectivity.

System Title	System Owner
Advanced Traceability and Control-Air Force	Air Force
Army Communication-Security Commodity Logistics Accounting Information Management System	Army
Aviation Maintenance Management Information System	Coast Guard
Centralized Integrated System – International Logistics System	Army
Combat Ammunition System	Air Force
Commodity Command Standard System	Army
Construction Battalion Center Supply System	Navy
Continuing Balancing System-Expanded	Army
Corps of Engineers Financial Management System	DFAS[1]
Defense Business Management System	DFAS[1]
Department of Defense Activity Address Directory	Army
Financial Inventory Accounting and Billing System	DFAS[1]
Finance Center	Coast Guard
Global Transportation Network	Air Force
Integrated Technical Item Management and Procurement System	Navy
Joint Ammunition Management Standard System	Air Force
Joint Computer-Aided Acquisition and Logistics Support	Army
Logistics Intelligence File	Army
Maintenance Resource Management System – Intermediate Maintenance Activity Component	Navy
Management Information System for International Logistics	DSCA[2]
Marine Air Ground Task Force – Data Library	Marine
Marine Corps Automated Digital Network Breakout System	Marines
Message Accountability and Delivery System	DLA
Military Supply and Transportation Evaluation Procedures	Army
National Guard Bureau	National Guard
Naval Medical Information Management Center	Navy
Naval Research Laboratory Financial Information Management System	DFAS

Note: See footnotes on last page of appendix.

System Title	System Owner
Navy Industrial Materials Management Systems	Navy
Other War Material Requirements for Other Services, D072	Air Force
Residual Asset Management	Navy
Single Stock Fund System	Army
Standard Accounting Budgeting and Reporting System	DFAS[1]
Standard Accounting and Reporting System	DFAS[1]
Standard Army Ammunition System	Army
Standard Army Retail Supply System	Army
Standard Base Supply System	Air Force
Standard Base Supply System Accounting and Finance	DFAS[1]
Standard Depot System	Army
Standard Material Accounting System	Air Force
Standard Finance System	DFAS[1]
Stock Control and Distribution System, D035K	Air Force
Stock Control and Distribution System, D035R	Air Force
Stock Control and Distribution System, D035T	Air Force
Streamlined Alternative Logistics Transmission System	Navy
Tandem	Navy
Technical Data Management System	Marine
Theater Army Medical Management Information System	Army
Uniform Automated Data Processing System	Navy
Uniform Inventory Control Program Alternate Transition System	Navy
Worldwide Port System	Army

[1]Defense Finance and Accounting Service.
[2]Defense Security Cooperation Agency.

Appendix D. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition and Technology
  Deputy Under Secretary of Defense (Logistics)
  Director, Defense Logistics Studies Information Exchange
  Director, Defense Procurement
Under Secretary of Defense (Comptroller)
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
  Deputy Assistant Secretary of Defense (Command, Control, Communications, Intelligence, Surveillance, Reconnaissance, and Space Systems)
  Deputy Chief Information Officer and Deputy Assistant Secretary of Defense (Chief Information Officer Policy and Implementation)
Assistant Secretary of Defense (Public Affairs)

Joint Staff

Director, Joint Staff

Department of the Army

Assistant Secretary of the Army (Financial Management and Comptroller)
Auditor General, Department of the Army
Inspector General, Department of the Army
Chief Information Officer, Army

Department of the Navy

Assistant Secretary of the Navy (Financial Management and Comptroller)
Auditor General, Department of the Navy
Inspector General, Department of the Navy
Chief Information Officer, Navy

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Auditor General, Department of the Air Force
Inspector General, Department of the Air Force
Chief Information Officer, Air Force

Other Defense Organizations

Director, Defense Contract Audit Agency
Director, Defense Information Systems Agency
  Inspector General, Defense Information Systems Agency
  Chief Information Officer, Defense Information Systems Agency
  United Kingdom Liaison Office, Defense Information Systems Agency
Director, Defense Logistics Agency
  Director, Defense Logistics Agency Systems Design Center
  Director, Defense Automatic Addressing System Center
Director, National Security Agency
  Inspector General, National Security Agency
Inspector General, Defense Intelligence Agency

Non-Defense Federal Organizations and Individuals

Office of Management and Budget
  Office of Information and Regulatory Affairs
General Accounting Office
  National Security and International Affairs Division
    Technical Information Center
  Accounting and Information Management Division
    Director, Defense Information and Financial Management Systems

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member (cont'd)

House Subcommittee on Government Management, Information, and Technology, Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform

Defense Logistics Agency Comments

DEFENSE LOGISTICS AGENCY
HEADQUARTERS
8725 JOHN J. KINGMAN ROAD, SUITE 2533
FT. BELVOIR, VIRGINIA 22060-6221

IN REPLY REFER TO

JAN 12 1999

DDAI

MEMORANDUM FOR ASSISTANT INSPECTOR GENERAL FOR AUDITING
DEPARTMENT OF DEFENSE

SUBJECT: Draft report on Year 2000 Computing Issues Related to the Defense Automatic Addressing System Center, 8LD-9021.01

Enclosed are DLA comments in response to your request of 30 November1998. If you have any questions, please notify Peggy Hayes, 767-6262.

JEFFREY GOLDSTEIN
Chief (Acting), Internal Review Office

Encl

cc:
CI
CIC

JAN 12 1999

SUBJECT: Year 2000 Computing Issues Related to the Defense Automatic Addressing System Center (Project NO. 8LD-9021.01)

FINDING: Status of the Defense Automatic Addressing System Center Year 2000 Program. The DLA and DAASC have taken positive actions to identify and correct Y2K problems with DAASC AISs. However, the DAASC contingency plan needed to address alternative procedures for continuity of operations of its core mission and to describe how it would preserve data for its mission-critical AISs. DAASC also needed to include the FAR Y2K-compliant language in its information technology contracts. Such actions were needed immediately to ensure that DLA would be able to perform its core supply mission without interruption after the year 1999.

DLA COMMENTS: DLA concurs.

RECOMMENDATION 1: We recommend that the Director, Defense Automatic Addressing Center prepare contingency plans in accordance with the requirements and guidelines in the DoD Year 2000 Management Plan to include addressing workarounds and data preservation.

DLA COMMENTS: Concur. DAASC has added data preservation strategy to its contingency plan. Full file backups are performed weekly and incremental backups are performed daily. This strategy was already part of the normal DAASC operations. For MILS customers, DAASC has included the following workarounds in the contingency plan. DAASC will advise customers to submit emergency requisitions through the Emergency Supply Operation Center (ESOC) or through the Defense Logistics Agency emergency Supply Expert System (DESEX). DAASC is recommending customers preposition materials prior to December 31, 1999, within cost reasonableness. DAASC is sending notifications to MILS and EDI customers. These notifications will be sent quarterly thru 1st Fiscal Quarter of 2000.

DISPOSITION: Action is Ongoing. ECD: 1st Fiscal Quarter 2000

RECOMMENDATION 2: We recommend that the Director, Defense Automatic Addressing Center include Federal Acquisition Regulation year 2000 compliance language in all open contracts for the purchase of information technology products, including software.

DLA COMMENTS: Concur. To date 35 out of the 40 contracts have had the clause added. The remaining contracts are scheduled to be completed by January 15, 1999.

DISPOSITION: Action is ongoing. ECD: January 15, 1999

ACTION OFFICER: Clarence McNeill, CIC, 767-2181
REVIEW/APPROVAL: Carla A. von Bernewitz, Chief Information Officer, CI, 30 Dec 98
COORDINATION: Peggy Hayes, DDAI

DLA APPROVAL:

(signed)
E.R. CHAMBERLIN
Rear Admiral, SC, USN
Deputy Director

Audit Team Members

This report was prepared by the Readiness and Logistics Support Directorate, Office of the Assistant Inspector General for Auditing, DoD

Shelton R. Young
Raymond D. Kidd
Hassan A. Soliman
Donney J. Bibb
Barry M. Johnson
Oscar I. San Mateo